On Universally Decodable Matrices for Space-Time Coding

Pascal O. Vontobel[1]
Department of EECS
Massachusetts Institute of Technology
Cambridge, MA 02139, USA
pascal.vontobel@ieee.org

Ashwin Ganesan
Department of ECE
University of Wisconsin-Madison
Madison, WI 53706, USA
ganesan@cae.wisc.edu

***Abstract*— The notion of universally decodable matrices (UDMs) was recently introduced by Tavildar and Viswanath while studying slow fading channels. It turns out that the problem of constructing UDMs is tightly connected to the problem of constructing maximum distance separable (MDS) codes. In this paper, we first study the properties of UDMs in general and then we discuss an explicit construction of a class of UDMs, a construction which can be seen as an extension of Reed-Solomon codes. In fact, we show that this extension is, in a sense to be made more precise later on, unique. Moreover, the structure of this class of UDMs allows us to answer some open conjectures by Tavildar, Viswanath, and Doshi in the positive, and it also allows us to formulate an efficient decoding algorithm for this class of UDMs. It turns out that our construction yields a coding scheme that is essentially equivalent to a class of codes that was proposed by Rosenbloom and Tsfasman. Moreover, we point out connections to so-called repeated-root cyclic codes.**

I. Introduction

Let L, N, and K be positive integers, let q be a prime power, let $[M] \triangleq \{0, \ldots, M-1\}$ for any positive integer M, and let $[M] \triangleq \{\,\}$ for any non-positive integer M. While studying slow fading channels (c.f. e.g. [1]), Tavildar and Viswanath [2] introduced the communication system shown in Fig. 1 which works as follows. An information (column) vector $\mathbf{u} \in \mathbb{F}_q^K$ is encoded into codeword vectors $\mathbf{x}_\ell \triangleq \mathbf{A}_\ell \cdot \mathbf{u} \in \mathbb{F}_q^N$, $\ell \in [L]$, where $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ are L matrices over $\mathbb{F}_q$ and of size $N \times K$. (Actually, Tavildar and Viswanath [2] considered only the special case $K = N$.) Upon sending $\mathbf{x}_\ell$ over the ℓ-th channel we receive $\mathbf{y}_\ell \in (\mathbb{F}_q \cup \{?\})^N$, where the question mark denotes an erasure. The channels are such that the received vectors $\mathbf{y}_0, \ldots, \mathbf{y}_{L-1}$ can be characterized as follows: there are integers $\upsilon_0, \ldots, \upsilon_{L-1}$, $0 \leq \upsilon_\ell \leq N$, $\ell \in [L]$ (that can vary from transmission to transmission) such that the first υ_ℓ entries of $\mathbf{y}_\ell$ are non-erased and agree with the corresponding entries of $\mathbf{x}_\ell$ and such that the last $N - \upsilon_\ell$ entries of $\mathbf{y}_\ell$ are erased.

Based on the non-erased entries we would like to reconstruct $\mathbf{u}$. The obvious decoding approach works as follows: construct a $(\sum_{\ell \in [L]} \upsilon_\ell) \times K$-matrix $\mathbf{A}$ that stacks the υ_0 first rows of $\mathbf{A}_0$, ..., the υ_{L-1} first rows of $\mathbf{A}_{L-1}$; then construct a length-$(\sum_{\ell \in [L]} \upsilon_\ell)$ vector $\mathbf{y}$ that concatenates the υ_0 first entries of $\mathbf{y}_0$, ..., the υ_{L-1} first entries of $\mathbf{y}_{L-1}$; finally, the vector $\hat{\mathbf{u}}$ is given as the solution of the linear equation system $\mathbf{A} \cdot \hat{\mathbf{u}} = \mathbf{y}$. Since $\mathbf{u}$ is arbitrary in $\mathbb{F}_q^K$, a necessary condition for successful decoding is that $\sum_{\ell \in [L]} \upsilon_\ell \geq K$. Because we would like to be able to decode correctly for all L-tuples $(\upsilon_0, \ldots, \upsilon_{L-1})$ that satisfy this necessary condition, we must guarantee that the matrix $\mathbf{A}$ has full rank for all possible L-tuples $(\upsilon_0, \ldots, \upsilon_{L-1})$ with $\sum_{\ell \in [L]} \upsilon_\ell \geq K$. Matrices that fulfill this condition are called universally decodable matrices (UDMs).

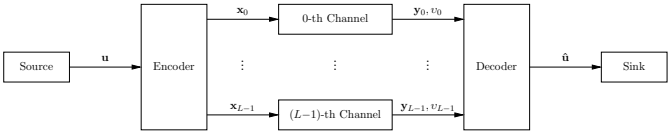

Fig. 1. Communication system with L parallel channels.

There is a tight connection between UDMs and maximum-distance separable (MDS) codes [3, Ch. 11]. More precisely, assume that $L \geq K$ and consider the $L \times K$-matrix $\mathbf{G}$ that consists of the zeroth row of $\mathbf{A}_0$, ..., the zeroth row of $\mathbf{A}_{L-1}$. Considering the above full-rank condition in all the cases where $(\upsilon_0, \ldots, \upsilon_{L-1})$ is such that $\sum_{\ell \in [L]} \upsilon_\ell = K$ and such that $0 \leq \upsilon_\ell \leq 1$ for all $\ell \in [L]$, we see that all $K \times K$ sub-matrices of $\mathbf{G}$ must have full rank. However, Th. 1 in [3, Ch. 11] implies that $\mathbf{G}$ must be the generator matrix of a q-ary MDS code of length L and dimension K.

Given the definition of UDMs, there are several immediate questions. For what values of L, N, K, and q do such matrices exist? What are the properties of these matrices? How can one construct such matrices? In [2] a construction is given for $L = 3$, any N, $K = N$, and $q = 2$. Doshi [4] gave a construction for $L = 4$, $N = K = 3$, and $q = 3$ and conjectured a construction for $L = 4$, N any power of 3, $K = N$, and $q = 3$. Ganesan and Boston [5] showed that for any $N \geq 2$, $K = N$, the value L is upper bounded by $L \leq q + 1$ and conjectured that this condition is also sufficient; in [6], [7] this conjecture was resolved, which settled the existence and construction questions for the special case $K = N$. In this paper we generalize this bound to the case $K \leq 2N$ and we will give an explicit construction that works for any positive integers L, N, K and any prime power q as long as

[1]The work for this paper was mainly done while being at Dept. of ECE, University of Wisconsin-Madison, Madison, WI 53706, USA.

$L \leq q+1$. In other words, this construction achieves for any $K \leq 2N$, $N \geq 2$, and any prime power q the above-mentioned upper bound on L. As a side result, our construction shows that the above-mentioned conjecture is indeed true. We will also show that for $K = N$ this construction is (in a sense to be made more precise) the unique possible way to extend a Reed-Solomon code (which is an MDS code) to UDMs. Finally, we will present an efficient decoding algorithm for the UDMs given by the above-mentioned construction; i.e. we will present an algorithm that efficiently solves $\mathbf{A} \cdot \hat{\mathbf{u}} = \mathbf{y}$.

We will point out several connections to other codes. As already mentioned, there is a tight connection between UDMs and MDS codes, but we will also point out an interesting relationship to so-called repeated-root cyclic codes. Moreover, it turns out that the above-mentioned construction of UDMs is essentially equivalent to so-called Reed-Solomon m-codes, a class of codes described by Rosenbloom and Tsfasman [8, Sec. 3]. These authors were interested in coding under a non-Hamming metric, namely a metric they called the m-metric and that is now also known as the Rosenbloom-Tsfasman metric. For this metric, Rosenbloom and Tsfasman show that the Reed-Solomon m-codes achieve the Singleton bound.

The paper is structured as follows. In Sec. II we properly define UDMs, in Sec. III we show how UDMs can be modified to obtain new UDMs, and in Sec. IV we discuss necessary conditions for the existence of UDMs. Sec. V is the main section where an explicit construction of UDMs is presented. More results (especially an efficient decoding algorithm) and all proofs will be presented in a forthcoming journal paper. (Note that some of the proofs are already available in a technical report, cf. [6].)

II. Universally Decodable Matrices

The notion of universally decodable matrices (UDMs) was introduced by Tavildar and Viswanath [2]. Before we give the definition of UDMs, let us agree on some notation. For any positive integer K, we let $\mathbf{I}_K$ be the $K \times K$ identity matrix and we let $\mathbf{J}_K$ be the $K \times K$ matrix where all entries are zero except for the anti-diagonal entries that are equal to one. For any positive integers N and K with $N \leq K$ we let $\mathbf{I}_{N,K}$ and $\mathbf{J}_{N,K}$ be the first K rows of $\mathbf{I}_K$ and $\mathbf{J}_K$, respectively. Row and column indices of matrices will always be counted from zero on and the entry in the i-th row and j-th column of a matrix $\mathbf{A}$ will be denoted by $[\mathbf{A}]_{i,j}$. Similarly, indices of vectors will be counted from zero on and the i-th entry of a vector $\mathbf{a}$ will be denoted by $[\mathbf{a}]_i$. For any positive integer L, N, and K, and any non-negative integer N we define the sets

$$\Upsilon^{=K}_{L,N} \triangleq \left\{ (\upsilon_0, \ldots, \upsilon_{L-1}) \;\middle|\; \begin{array}{l} 0 \leq \upsilon_\ell \leq N, \ell \in [L], \\ \sum_{\ell \in [L]} \upsilon_\ell = K \end{array} \right\},$$

$$\Upsilon^{\geq K}_{L,N} \triangleq \left\{ (\upsilon_0, \ldots, \upsilon_{L-1}) \;\middle|\; \begin{array}{l} 0 \leq \upsilon_\ell \leq N, \ell \in [L], \\ \sum_{\ell \in [L]} \upsilon_\ell \geq K \end{array} \right\}.$$

Definition 1 *Let N, K, and L be some positive integers and let q be a prime power. The L matrices $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ over $\mathbb{F}_q$ and of size $N \times K$ are (L, N, K, q)-UDMs, or simply UDMs, if for every $(\upsilon_0, \ldots, \upsilon_{L-1}) \in \Upsilon^{\geq K}_{L,N}$ they fulfill the UDMs condition which says that the $(\sum_{\ell \in [L]} \upsilon_\ell) \times K$ matrix composed of the first υ_0 rows of $\mathbf{A}_0$, the first υ_1 rows of $\mathbf{A}_1$, ..., the first υ_{L-1} rows of $\mathbf{A}_{L-1}$ has full rank.* □

In the following we will only consider (L, N, K, q)-UDMs for which $N \leq K \leq LN$ holds.[2] We list some immediate consequences of the above definition.

- To assess that some matrices $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ are UDMs, it is sufficient to check the UDMs condition only for every $(\upsilon_0, \ldots, \upsilon_{L-1}) \in \Upsilon^{=K}_{L,N}$. In the case $K = N$ there are $\binom{N+L-1}{L-1}$ such L-tuples.
- If the matrices $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ are UDMs then all these matrices have full rank.
- If the matrices $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ are (L, N, K, q)-UDMs then they are (L, N, K, q')-UDMs for any q' that is a power of q.
- Let σ be any permutation of $[L]$. If the matrices $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ are (L, N, K, q)-UDMs then the matrices $\mathbf{A}_{\sigma(0)}, \ldots, \mathbf{A}_{\sigma(L-1)}$ are also (L, N, K, q)-UDMs.
- If the matrices $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ are (L, N, K, q)-UDMs then the matrices $\mathbf{A}_0, \ldots, \mathbf{A}_{L'-1}$ are (L', N, K, q)-UDMs for any positive L' with $L' \leq L$. (Note that the condition $K \leq L'N$ may be violated.)
- If the matrices $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ are (L, N, K, q)-UDMs and $\mathbf{B}$ is an invertible $K \times K$-matrix over $\mathbb{F}_q$ then the matrices $\mathbf{A}_0 \cdot \mathbf{B}, \ldots, \mathbf{A}_{L-1} \cdot \mathbf{B}$ are (L, N, K, q)-UDMs. Without loss of generality, we can therefore assume that $\mathbf{A}_0 = \mathbf{I}_{N,K}$.
- For $K = 1$ (note that we must have $N = 1$ because we assume that $N \leq K$) we see that for any positive integer L and any prime power q, the L matrices $(1), \ldots, (1)$ are $(L, N{=}1, K{=}1, q)$-UDMs. Because of the trivial-ness of the case $K = 1$, the rest of the paper focuses on the case $K \geq 2$.

Example 2 Let N be any positive integer, let q be any prime power, and let $L \triangleq 2$. Let $\mathbf{A}_0 \triangleq \mathbf{I}_N$ and let $\mathbf{A}_1 \triangleq \mathbf{J}_N$. It can easily be checked that $\mathbf{A}_0, \mathbf{A}_1$ are $(L{=}2, N, K{=}N, q)$-UDMs. Indeed, let for example $N \triangleq 5$. We must check that for any non-negative integers υ_1 and υ_2 such that $\upsilon_1 + \upsilon_2 = 5$ the UDMs condition is fulfilled. E.g. for $(\upsilon_1, \upsilon_2) = (3, 2)$ we must show that the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

has rank 5, which can easily be verified. □

[2] The reason for the first inequality is that for the purpose of unique decodability it does not help to send more than K symbols over the ℓ-th channel, $\ell \in [L]$. (This condition might be weakened though for channel models that introduce not only erasures but also errors.) The reason for the second inequality is that if $K > LN$ then we will never receive enough symbols to decode uniquely. Note that for $K = N$, i.e. the case studied by Tavildar and Viswanath [2], both conditions in $N \leq K \leq LN$ are fulfilled for any positive L.

Example 3 In order to give the reader a feeling how UDMs might look like for $L > 2$, we give here a simple example for $L = 4$, $N = K = 3$, and $q = 3$, namely

$$\mathbf{A}_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{A}_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$
$$\mathbf{A}_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{A}_3 = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

One can verify that for all $(\upsilon_0, \upsilon_1, \upsilon_2, \upsilon_3) \in \Upsilon_{4,3}^{=3}$ (there are 20 such four-tuples) the UDMs condition is fulfilled and hence the above matrices are indeed UDMs. For example, for $(\upsilon_0, \upsilon_1, \upsilon_2, \upsilon_3) = (0, 0, 3, 0)$, $(\upsilon_0, \upsilon_1, \upsilon_2, \upsilon_3) = (0, 0, 1, 2)$, and $(\upsilon_0, \upsilon_1, \upsilon_2, \upsilon_3) = (1, 1, 0, 1)$ the UDMs condition means that we have to check if the matrices

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 1 \end{pmatrix}$$

have rank 3, respectively, which is indeed the case. Before concluding this example, let us remark that the above UDMs are the same UDMs that appeared in [4] and [2, Sec. 4.5.4]. □

III. Modifying UDMs

This section shows how UDMs can be modified to obtain new UDMs.

Lemma 4 *Let $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ be (L, N, K, q)-UDMs. For any $\ell \in [L]$ and $n \in [N]$ we can replace the n-th row of $\mathbf{A}_\ell$ by any non-zero multiple of itself without violating any UDMs condition. Moreover, for any $\ell \in [L]$ and $n, n' \in [N]$, $n > n'$, we can add any multiples of the n'-th row of $\mathbf{A}_\ell$ to the n-th row of $\mathbf{A}_\ell$ without violating any UDMs condition. More generally, the matrix $\mathbf{A}_\ell$ can be replaced by $\mathbf{C}_\ell \cdot \mathbf{A}_\ell$ without violating any UDMs condition, where $\mathbf{C}_\ell$ is an arbitrary lower triangular $N \times N$-matrix over $\mathbb{F}_q$ with non-zero diagonal entries.*

Lemma 5 *Let $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ be (L, N, K, q)-UDMs. Then there exist matrices $\mathbf{A}'_0, \ldots, \mathbf{A}'_{L-1}$ that are (L, N, K, q)-UDMs and where for all $\ell' \in \lfloor L/2 \rfloor$ the the n-th row of $\mathbf{A}'_{2\ell'}$ equals the $(K-1-n)$-th row of $\mathbf{A}'_{2\ell'+1}$ for all $K - N \leq n \leq N - 1$. In the case $K = N$ this means that for all $\ell' \in \lfloor L/2 \rfloor$ the matrix $\mathbf{A}'_{2\ell'+1}$ is the same as $\mathbf{A}'_{2\ell'}$ except that the rows are in reversed order, i.e. $\mathbf{A}_{2\ell'+1} = \mathbf{J}_N \cdot \mathbf{A}'_{2\ell'}$.*

Remark 6 From Lemma 5 we see that when considering (L, N, K, q)-UDMs $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ we can without loss of generality assume that $\mathbf{A}_0 = \mathbf{I}_{N,K}$ and that $\mathbf{A}_1 = \mathbf{J}_{N,K}$. □

IV. Necessary Conditions for Existence of UDMs

The above lemmas can be used to obtain conditions for the existence of UDMs.

Lemma 7 *Let q be a prime power. If $K \geq 2$ then $(L, N, K \leq 2N, q)$-UDMs can only exist for $L \leq q + 1$. (Note that this upper bound on L is independent of N and K as long as $2 \leq K \leq 2N$.)*

Lemma 8 *Let q be a prime power. Then $(L, N, K = 2N+1, q)$-UDMs can only exist for $L \leq q + 2$. (Note that this upper bound on L is independent of N.)*

Note that Lemmas 7 and 8 are generalizations of a result in [5], [7] that dealt with the case $K = N$. Prop. 12 will show that the upper bound on L in Lemma 7 is the best possible because for any $L \leq q+1$ we can explicitly construct $(L, N, K \leq 2N, q)$-UDMs. Moreover, as Rem. 9 shows, the upper bound on L in Lemma 8 is the best possible if no further restrictions on N and q are imposed.

Remark 9 Let $q \triangleq 2^s$ for some integer s and let α be a primitive element in $\mathbb{F}_q$, i.e. α is an $(q-1)$-th primitive root of unity. From [3, Th. 10 in Ch. 11] it follows that the matrices

$$\begin{aligned} \mathbf{A}_0 &\triangleq \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \\ \mathbf{A}_1 &\triangleq \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}, \\ \mathbf{A}_{\ell+2} &\triangleq \begin{pmatrix} 1 & \alpha^\ell & \alpha^{2\ell} \end{pmatrix} \quad \text{for } 0 \leq \ell \leq q-2, \\ \mathbf{A}_{q+1} &\triangleq \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

are $(q+2, 1, 3, q)$-UDMs. Similarly, [3, Th. 10 in Ch. 11] shows that there are $(q+2, 1, (q+2)-3, q)$-UDMs. □

For $K > 2N + 1$ it is more complicated to find an upper bound on L in terms of q. In particular, for $N = 1$ the question of finding upper bounds on L is equivalent to the question of the existence of MDS codes [3, Ch. 11]: it is conjectured that for $2 \leq K \leq L - 2$ we must have $L \leq q + 1$. (The only known exception to this conjecture are MDS codes of length $L = q + 2$ and dimension $K = 3$ or $K = L - 3$ for $q = 2^s$ where s is some positive integer, cf. Rem. 9.)

V. An Explicit Construction of UDMs

In this section we would like to present an explicit construction of (L, N, K, q)-UDMs, cf. Prop. 12 and Cor. 13. This construction is very much motivated by the connection of UDMs to MDS codes mentioned in Sec. I and the fact that Reed-Solomon codes are MDS codes. In fact, we will see in Prop. 15 that there is (in a sense to be made more precise) only one possible way to construct UDMs based on Reed-Solomon codes.

Before we proceed, we need some definitions. First, whenever necessary we use the natural mapping of the integers into the prime subfield[3] of $\mathbb{F}_q$. Secondly, we define the binomial coefficient $\binom{a}{b}$ in the usual way. Note that $\binom{a}{b} = 0$ for all $a < b$.

Definition 10 *Let $a(\mathsf{X}) \triangleq \sum_{k=0}^{d} a_k \mathsf{X}^k \in \mathbb{F}_q[\mathsf{X}]$ be a polynomial and let $\beta \in \mathbb{F}_q$. The Taylor polynomial expansion of $a(\mathsf{X})$ around $\mathsf{X} = \beta$ is defined to be $a(\mathsf{X}) = \sum_{n=0}^{d} a_{\beta,n} (\mathsf{X} - \beta)^n \in$*

[3] When $q = p^s$ for some prime p and some positive integer s then $\mathbb{F}_p$ is a subfield of $\mathbb{F}_q$ and is called the prime subfield of $\mathbb{F}_q$. $\mathbb{F}_p$ can be identified with the integers where addition and multiplication are modulo p.

$\mathbb{F}_q[\mathsf{X}]$ *for suitably chosen* $a_{\beta,n} \in \mathbb{F}_q$, $0 \leq i \leq d$, *such that equality holds.* □

It can be verified that the Taylor polynomial coefficients $a_{\beta,n}$ can be expressed using Hasse derivatives[4] of $a(\mathsf{X})$, i.e. $a_{\beta,n} = a^{(n)}(\beta) = \sum_{k=0}^{d} a_k \binom{k}{n} \beta^{k-n}$. On the other hand, the coefficients of $a(\mathsf{X})$ can be expressed as $a_k = \sum_{n=0}^{d} a_{\beta,n} \binom{n}{k} (-\beta)^{n-k}$.

Lemma 11 *Let* $a(\mathsf{X}) \triangleq \sum_{k=0}^{d} a_k \mathsf{X}^k \in \mathbb{F}_q[\mathsf{X}]$ *be a non-zero polynomial, let* $\beta \in \mathbb{F}_q$, *and let* $a(\mathsf{X}) = \sum_{n=0}^{d} a_{\beta,n} (\mathsf{X}-\beta)^n \in \mathbb{F}_q[\mathsf{X}]$ *be the Taylor polynomial expansion of* $a(\mathsf{X})$ *around* $\mathsf{X} = \beta$. *The polynomial* $a(\mathsf{X})$ *has a zero at* $\mathsf{X} = \beta$ *of multiplicity* m *if and only if* $a_{\beta,n} = 0$ *for* $0 \leq n < m$ *and* $a_{\beta,n} \neq 0$.

In the following, evaluating the n-th Hasse derivative $u^{(n)}(\mathsf{L})$ of a polynomial $u(\mathsf{L})$ at $\mathsf{L} = \infty$ shall result in the value u_{K-1-n}, i.e. we set $u^{(n)}(\infty) \triangleq u_{K-1-n}$.

Proposition 12 *Let* N *and* K *be some positive integers, let* q *be some prime power, and let* α *be a primitive element in* $\mathbb{F}_q$. *If* $L \leq q+1$ *then the following* L *matrices over* $\mathbb{F}_q$ *of size* $N \times K$ *are* (L, N, K, q)*-UDMs:*

$$\mathbf{A}_0 \triangleq \mathbf{I}_{N,K}, \quad \mathbf{A}_1 \triangleq \mathbf{J}_{N,K}, \quad \mathbf{A}_2, \quad \ldots, \quad \mathbf{A}_{L-1}, \text{ where}$$

$$[\mathbf{A}_{\ell+2}]_{n,k} \triangleq \binom{k}{n} \alpha^{\ell(k-n)}, \ (\ell, n, k) \in [L-2] \times [N] \times [K].$$

Note that $\binom{k}{n}$ *is to be understood as follows: compute* $\binom{k}{n}$ *over the integers and apply only then the natural mapping to* $\mathbb{F}_q$.

Corollary 13 *Let us associate the information polynomial* $u(\mathsf{L}) \triangleq \sum_{k \in [K]} u_k \mathsf{L}^k \in \mathbb{F}_q[\mathsf{L}]$ *with* $u_k \triangleq [\mathbf{u}]_k$, $k \in [K]$, *to the information vector* $\mathbf{u}$. *The construction in the above proposition results in a coding scheme where the vector* $\mathbf{u}$ *is mapped to the vectors* $\mathbf{x}_0, \ldots, \mathbf{x}_{L-1}$ *with entries*

$$[\mathbf{x}_\ell]_n = u^{(n)}(\beta_\ell), \quad (\ell, n) \in [L] \times [N],$$

where $\beta_0 \triangleq 0$, $\beta_1 \triangleq \infty$, $\beta_{\ell+2} \triangleq \alpha^\ell$, $\ell \in [L-2]$. *(Note that because* α *is a primitive element of* $\mathbb{F}_q$, *all* β_ℓ, $\ell \in [L]$, *are distinct.) This means that over the* ℓ*-th channel we are transmitting the coefficients of the Taylor polynomial expansion of* $u(\mathsf{L})$ *around* $\mathsf{L} = \beta_\ell$.

Example 14 For $N \triangleq 3$, $K \triangleq N$, $p \triangleq 3$, and $\alpha \triangleq 2$, we obtain the $L = 3 + 1 = 4$ matrices that were shown in Ex. 3. Note that $\mathbf{A}_3$ is nearly the same as $\mathbf{A}_2$: it differs only in that the main diagonal is multiplied by $\alpha^0 = 1$, the first upper diagonal is multiplied by $\alpha^1 = 2$, the second upper diagonal is multiplied by $\alpha^2 = 1$, the first lower diagonal is multiplied by $\alpha^{-1} = 2$, and the second lower diagonal is multiplied by $\alpha^{-2} = 1$. □

[4]Hasse derivatives were introduced in [9]. For any non-negative integer i, the i-th Hasse derivative of a polynomial $a(\mathsf{X}) \triangleq \sum_{k=0}^{d} a_k \mathsf{X}^k \in \mathbb{F}_q[\mathsf{X}]$ is defined to be $a^{(i)}(\mathsf{X}) \triangleq \sum_{k=0}^{d} \binom{k}{i} a_k \mathsf{X}^{k-i}$.

We collect some remarks about the UDMs constructed in Prop. 12 / Cor. 13.

- All matrices $\mathbf{A}_\ell$, $2 \leq \ell < L$, are upper triangular matrices with non-zero diagonal entries. This follows from the fact that $\binom{k}{n} = 1$ if $k = n$ and $\binom{k}{n} = 0$ if $k < n$.
- The matrix $\mathbf{A}_2$ is an upper triangular matrix where the non-zero part equals Pascal's triangle (modulo p), see e.g. $\mathbf{A}_2$ in Ex. 3. However, whereas usually Pascal's triangle is depicted such that the rows correspond to the upper entry in the binomial coefficient, here the columns of the matrix correspond to the upper entry in the binomial coefficient.
- As already mentioned in Sec. I, the construction of UDMs in Prop. 12 / Cor. 13 is essentially equivalent to codes presented by Rosenbloom and Tsfasman [8].[5] They were interested in the so-called m-metric which is now also known as the Rosenbloom-Tsfasman metric.[6] Later, Nielsen [10] discussed Sudan-type (error) decoding algorithms for these codes. Related work on codes under the Rosenbloom-Tsfasman metric include: Dougherty and Skriganov [13] on MacWilliams duality, Dougherty and Skriganov [13] and Dougherty and Shiromoto [14] on codes over rings and other generalized alphabets, Lee [15] on automorphisms that preserve the Rosenbloom-Tsfasman metric, Chen and Skriganov [16] on codes with large distances simultaneously in the Hamming and in the Rosenbloom-Tsfasman metric.
- There is also a connection between the construction of UDMs in Prop. 12 / Cor. 13 and so-called repeated-root cyclic codes [17], [18], [19], [20], i.e. the mathematics behind both of them is very similar. Repeated-root cyclic codes are cyclic codes where the generator polynomial has zeros with multiplicity possibly larger than one: Lemma 11, the lemma that is crucial for proving the UDMs property for the UDMs constructed in Prop. 12 / Cor. 13, was used by Castagnoli et al. [18] to formulate parity-check matrices for repeated-root cyclic codes.

Interestingly, for $K = N$ the construction in Prop. 12 / Cor. 13 is unique in a sense made more precise in the following lemma.

Proposition 15 *The construction in Prop. 12 is unique in the following sense. Let* N *be some positive integer, let* q *be some prime power, let* α *be a primitive element in* $\mathbb{F}_q$, *and let* L *be a positive integer with* $L \leq q+1$. *Moreover, let* $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$ *be* $(L, N, K{=}N, q)$*-UDMs as given by Prop. 12. (Note that the* $L \times N$ *matrix consisting of the zeroth rows of* $\mathbf{A}_0, \ldots, \mathbf{A}_{L-1}$

[5]Note that the communication system mentioned in Sec. 1 of [8] also talks about parallel channels: however, that communication system would correspond to (in our notation) sending L symbols over N channels. On the other hand, the communication system that is mentioned in Nielsen [10, Ex. 18] is more along the lines of the Tavildar-Viswanath channel model [2] mentioned in Sec. I.

[6]In the context of uniform distributions, this metric was then later on introduced independently by Martin and Stinson [11] and by Skriganov [12].

is the generator matrix of a Reed-Solomon code of length L and dimension $\min(N, L)$.)

Consider the $N \times N$ matrices $\mathbf{A}'_0, \ldots, \mathbf{A}'_{L-1}$ over $\mathbb{F}_q$ such that $\mathbf{A}'_0 \triangleq \mathbf{A}_0$, $\mathbf{A}'_1 \triangleq \mathbf{A}_1$, and where the zeroth row of $\mathbf{A}'_\ell$ matches the zeroth row of $\mathbf{A}_\ell$ for all $2 \leq \ell \leq L-1$. Modulo the modifications described in Lemma 4, the only way to fill the remaining entries of the matrices $\mathbf{A}'_0, \ldots, \mathbf{A}'_{L-1}$ such that they are $(L, N, K{=}N, q)$-UDMs is to choose $\mathbf{A}'_\ell = \mathbf{A}_\ell$ for all $2 \leq \ell \leq L-1$.

The above proposition says something about the uniqueness of UDMs if one bases the construction of UDMs on Reed-Solomon codes. The question is then how unique are Reed-Solomon codes in the class of MDS codes. In that respect, MacWilliams and Sloane [3, p. 330] note that if q is odd then in many (conjecturally all) cases there is an unique $[q{+}1, k, q{-}k+2]$ q-ary MDS code. But if q is even this is known to be false.

Corollary 16 *Consider the setup of Prop. 12 with $N = K = p^m$, where p is the characteristic of $\mathbb{F}_q$ and where m is some positive integer.*[7] *Let*

$$n = n_{m-1}p^{m-1} + \cdots + n_1 p + n_0, \quad 0 \leq n_h < p,\ h \in [m],$$
$$k = k_{m-1}p^{m-1} + \cdots + k_1 p + k_0, \quad 0 \leq k_h < p,\ h \in [m]$$

be the radix-p representations of $n \in [N]$ and $k \in [N]$, respectively. Then the entries of $\mathbf{A}_{\ell+2}$, $\ell \in [L-2]$, can be written as

$$[\mathbf{A}_{\ell+2}]_{n,k} = \prod_{h \in [m]} \binom{k_h}{n_h} \alpha^{\ell(k_h - n_h)p^h}.$$

This shows that the matrices $\mathbf{A}_\ell$, $\ell \in [L]$, can be written as tensor products of some $p \times p$ matrices. In the special case $q = p$ (i.e. q is a prime) we can say more. Namely, letting $\mathbf{A}'_0, \ldots, \mathbf{A}'_{L-1}$ be the $(p{+}1, p, p, p)$-UDMs as constructed in Prop. 12 we see that $\mathbf{A}_\ell = (\mathbf{A}'_\ell)^{\otimes m}$ for all $\ell \in [L]$.

Consider the same setup as in Cor. 16. Because $0 \leq n_h < p$, we observe that $\binom{k_h}{n_h}$ is a polynomial function of degree n_h in k_h. Using Lemma 4, the matrices can therefore be modified so that the entries are

$$[\mathbf{A}_{\ell+2}]_{n,k} = \prod_{h \in [m]} k_h^{n_h} \alpha^{\ell(k_h - n_h)p^h}, \ (\ell, n, k) \in [L-2] \times [N] \times [N].$$

Letting $q = p \triangleq 2$, $L \triangleq q + 1 = 3$, $N = K = 2^m$, and $\alpha \triangleq 1$ we have $[\mathbf{A}_2]_{n,k} = \prod_{h \in [m]} k_h^{n_h}$, which recovers the $(L{=}3, N{=}2^m, K{=}N, q{=}2)$-UDMs in [2, Sec. 4.5.3] since the latter matrix is a Hadamard matrix.

Recall the $(L{=}4, N{=}3, K{=}N, q{=}3)$-UDMs $\mathbf{A}_0, \ldots, \mathbf{A}_3$ from Ex. 3. The authors of [2], [4] conjecture that the tensor powers $\mathbf{A}_0^{\otimes m}, \ldots, \mathbf{A}_3^{\otimes m}$ are $(4, 3^m, 3^m, 3)$-UDMs for any positive integer m. This is indeed the case and can be shown as follows. From Ex. 14 we know that $\mathbf{A}_0, \ldots, \mathbf{A}_3$ can be obtained by the construction in Prop. 12. Because $q = 3$ is a prime, Cor. 16 yields the desired conclusion that the tensor powers $\mathbf{A}_0^{\otimes m}, \ldots, \mathbf{A}_3^{\otimes m}$ are $(4, 3^m, 3^m, 3)$-UDMs for any positive integer m.

[7] The statement in this corollary could be extended to more general setups but we will not do so.

Acknowledgments

The first author was supported by NSF Grants ATM-0296033 and DOE SciDAC and by ONR Grant N00014-00-1-0966. The second author was supported by NSF Grant CCF-0514801. We would like to thank Nigel Boston for general discussions on the topic, Ralf Koetter for pointing out to us the papers [8], [10], and Kamil Zigangirov for providing us with a copy of [8].

References

[1] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, UK: Cambridge University Press, 2005.

[2] S. Tavildar and P. Viswanath, "Approximately universal codes over slow fading channels," *accepted for IEEE Trans. Inform. Theory, available online under* `http://www.arxiv.org/abs/cs.IT/0512017v1` *and* `http://www.arxiv.org/abs/cs.IT/0512017v2`, Dec. 2005.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: North-Holland, 1977.

[4] V. Doshi, *Explicit permutation codes for the slow fading channel*. BS Thesis, ECE Dept., University of Illinois at Urbana-Champaign, 2005.

[5] A. Ganesan and N. Boston, "Universally decodable matrices," in *Proc. 43rd Allerton Conf. on Communications, Control, and Computing*, (Allerton House, Monticello, Illinois, USA), Sep. 28–30 2005. Available online under `http://www.math.wisc.edu/~boston/papers.html`.

[6] P. O. Vontobel and A. Ganesan, *An Explicit Construction of Universally Decodable Matrices*. Technical report, Aug. 2005. Available online under `http://www.arxiv.org/abs/cs.IT/0508098`.

[7] A. Ganesan and P. O. Vontobel, "On the existence of universally decodable matrices," *submitted to IEEE Trans. Inform. Theory, available online under* `http://www.arxiv.org/abs/cs.IT/0601066`, Jan. 2006.

[8] M. Y. Rosenbloom and M. A. Tsfasman, "Codes for the m-metric," *Probl. Inform. Transm.*, vol. 33, no. 1, pp. 45–52, 1997.

[9] H. Hasse, "Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik," *J. Reine. Ang. Math.*, vol. 175, pp. 50–54, 1936.

[10] R. R. Nielsen, "A class of Sudan-decodable codes," *IEEE Trans. on Inform. Theory*, vol. IT–46, no. 4, pp. 1564–1572, 2000.

[11] W. J. Martin and D. R. Stinson, "Association schemes for ordered orthogonal arrays and (T, M, S)-nets," *Canad. J. Math.*, vol. 51, no. 2, pp. 326–346, 1999.

[12] M. M. Skriganov, "Coding theory and uniform distributions," *Algebra i Analiz*, vol. 13, no. 2, pp. 191–239, 2001.

[13] S. T. Dougherty and M. M. Skriganov, "Maximum distance separable codes in the ρ metric over arbitrary alphabets," *J. Algebraic Combin.*, vol. 16, no. 1, pp. 71–81, 2002.

[14] S. T. Dougherty and K. Shiromoto, "Maximum distance codes in $\mathrm{Mat}_{n,s}(\mathbb{Z}_k)$ with a non-Hamming metric and uniform distributions," *Des. Codes Cryptogr.*, vol. 33, no. 1, pp. 45–61, 2004.

[15] K. Lee, "The automorphism group of a linear space with the Rosenbloom-Tsfasman metric," *European J. Combin.*, vol. 24, no. 6, pp. 607–612, 2003.

[16] W. W. L. Chen and M. M. Skriganov, "Explicit constructions in the classical mean squares problem in irregularities of point distribution," *J. Reine Angew. Math.*, vol. 545, pp. 67–95, 2002.

[17] C. L. Chen, *Some results on algebraically structured error-correcting codes*. PhD thesis, University of Hawii, Honolulu, HI, USA, 1969.

[18] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, "On repeated-root cyclic codes," *IEEE Trans. on Inform. Theory*, vol. IT–37, no. 2, pp. 337–342, 1991.

[19] J. H. van Lint, "Repeated-root cyclic codes," *IEEE Trans. on Inform. Theory*, vol. 37, no. 2, pp. 343–345, 1991.

[20] R. Morelos-Zaragoza, "A note on repeated-root cyclic codes," *IEEE Trans. on Inform. Theory*, vol. IT–37, no. 6, pp. 1736–1737, 1991.